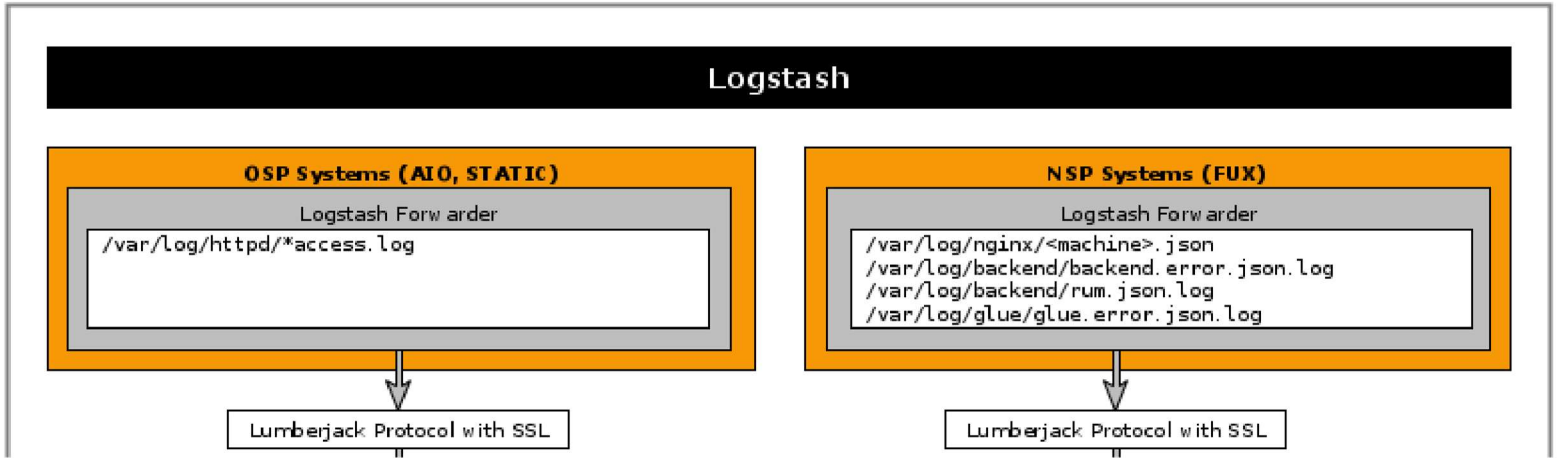
Logging-Dokumentation

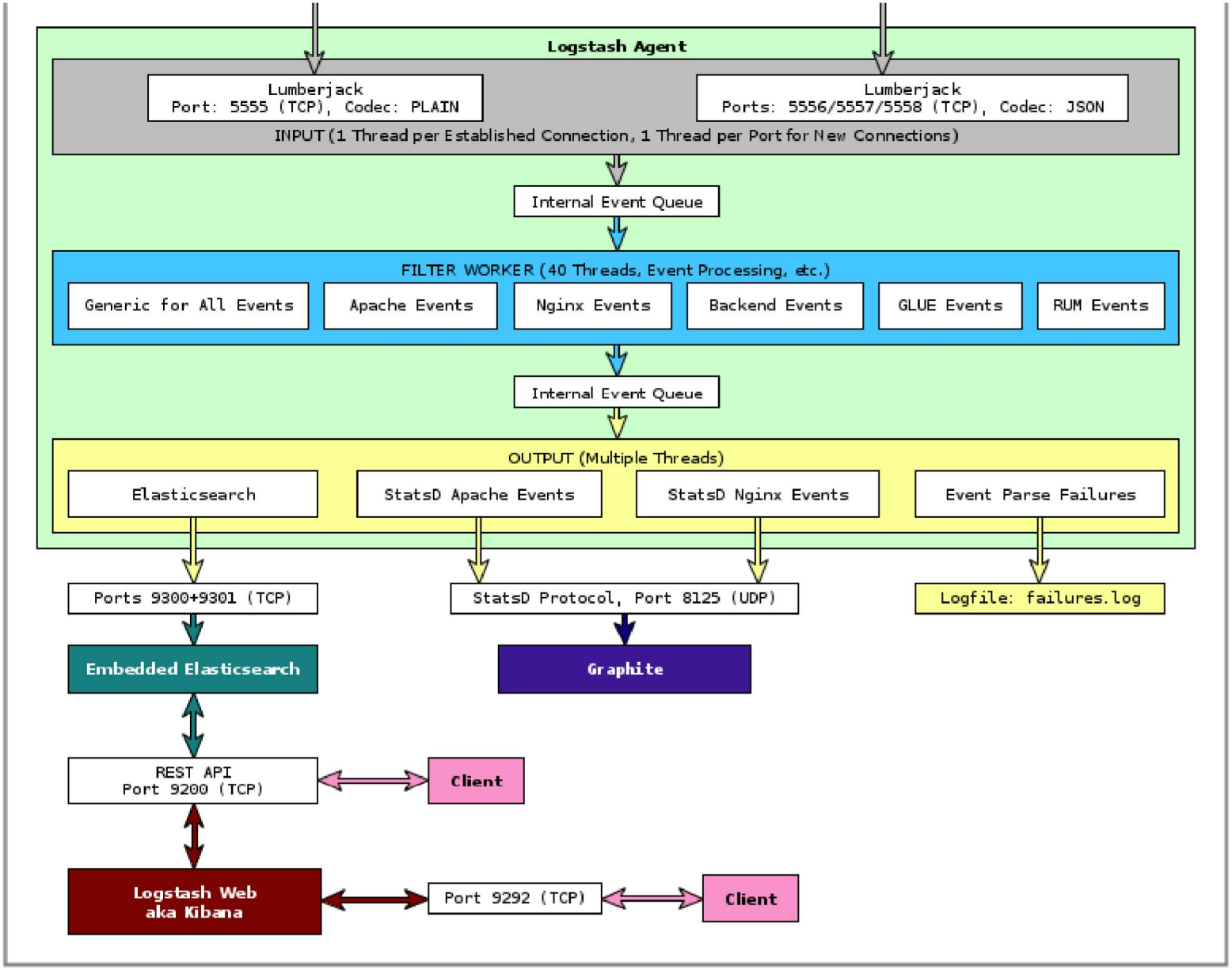
Aus bettermarks

Inhaltsverzeichnis

Logging bei bettermarks

Logging - Schematische Darstellung




Logstash Agent
Lumberjack
Port: 5555 (TCP), Codec: PLAIN
Lumberjack
Ports: 5556/5557/5558 (TCP), Codec: JSON
INPUT (1 Thread per Established Connection, 1 Thread per Port for New Connections)
Internal Event Queue
FILTER WORKER (40 Threads, Event Processing, etc.)
Generic for All Events
Apache Events
Nginx Events
Backend Events
GLUE Events
RUM Events
Internal Event Queue
OUTPUT (Multiple Threads)
Elasticsearch
StatsD Apache Events
StatsD Nginx Events
Event Parse Failures
Ports 9300+9301 (TCP)
StatsD Protocol, Port 8125 (UDP)
Logfile: failures.log
Embedded Elasticsearch
Graphite
REST API
Port 9200 (TCP)
Client
Logstash Web
aka Kibana
Port 9292 (TCP)
Client

Welche Loginformationen werden bei welchen Systemen erhoben?

OSP System (Benutzerverwaltung)

- Im Schuljahr 2016/2017 werden im OSP-System folgende Benutzerinformationen verwaltet:
  - Benutzername
  - Kennwort (als Hash-Wert)
  - Wenn vorhanden: Vor- und Zuname, E-Mail-Adresse
- Ab dem Schuljahr 2017/2018 soll hier ein neues System genutzt werden (Glue)
  - Es werden keine anderen Daten als beim OSP-System gespeichert
- Geloggt werden eingehende Anfragen vom Client-Computer auf dem Server und die entsprechenden Antworten (sogenannte Access-Logs)
- Geloggt wird im JavaScript Object Notation - Format (kurz JSON)
- In den Logs finden sich (abgesehen von der IP-Adresse) keinerlei personenbezogene Daten

NSP-System (das eigentliche Mathematik-Lernsystem)

- Geloggt werden eingehende Anfragen vom Client-Computer auf dem Server und die entsprechenden Antworten (sogenannte Access-Logs)
- Geloggt werden Server-Fehler (backend-Fehler)
- Geloggt werden ausgewählte Server-Ereignisse (backend-Logs)
- Geloggt wird im JavaScript Object Notation - Format (kurz JSON)
- In den Logs finden sich (abgesehen von der IP-Adresse) keinerlei personenbezogene Daten, diese kommen derzeit vom OSP (Benutzerverwaltung)
- Für Nutzerinnen und Nutzer aus Deutschland wird aktuell nicht das Glue-System (Benutzerverwaltung) verwendet

Übertragung der Logdaten zum Log-Server

- Die Log-Daten werden von den Systemen OSP und NSP HTTPS-Verschlüsselt (AES 2654 bit) an den Logstash-Server übertragen
- Hierfür wird das Netzwerk-Protokoll lumberjack und die Ports 5555, 5556, 5557 und 5558 genutzt
- Die Übertragung findet im bettermarks-eigenen VLAN beim Dienstleister UMC statt, ein Zugriff auf diesen Übertragungsvorgang von außen ist nicht möglich

Verarbeitung der Logdaten

- Der Logstash-Dienst nimmt die Logdaten entgegen
- Die ankommenden Log-Ereignisse (Events) werden entsprechend den definierten Kategorien verarbeitet
- Die verarbeiteten Ereignisse werden zur Ausgabe bereitgestellt

Ausgabe der Logdaten

- Auf dem Log-Server laufen zwei "Ausgabedienste": Elasticsearch und Graphite
- Elasticsearch ist eine Suchmaschine, welche ein Durchsuchen der Logdaten ermöglicht
  - Als Benutzeroberfläche für Elasticsearch läuft auf dem Log-Server Kibana
- Graphite visualisiert definierte Ereignisse im zeitlichen Verlauf nahezu in Echtzeit

Zugriff auf die Logdaten

- Eine Verbindung / ein Zugriff auf die Logdaten ist von außen nicht möglich
- Zugriff ist nur möglich von innerhalb des bettermarks-VLANs beim Dienstleister UMC bzw. mit einer entsprechenden VPN-Verbindung in das bettermarks-
- Netzwerk
- Der Kibana - Dienst auf dem Logstash-Server ist aus dem bettermarks-Netzwerk im Browser aufrufbar und Suchanfragen können gestellt werden
  Die Graphite - Dienst auf dem Logstash-Server ist aus dem bettermarks-Netzwerk im Browser aufrufbar und die definierten Visualisierungen können angezeigt werden

Speicher- und Löschfristen

- Die Log-Ereignisse auf dem OSP - und NSP - System werden auf diesen Systemen nach erfolgter Übertragung an den Logstash-Server unmittelbar automatisch gelöscht
- Sämtliche Log-Informationen mit einem Alter größer sieben Tage (Zeitstempel älter als sieben Tage) werden automatisch in den frühen Morgenstunden vom Log-Server gelöscht
- Ein eventuelles Löschen von Backups ist nicht nötig, da von den konkreten Log-Daten kein Backup vorgehalten wird